

Recipe 11 - Configuration Guide for Setting up HP Select Access 5.2 as an AA

Table of Contents

1	Setup	1
1.1	Terms and Introduction	1
1.2	Using the Setup Tool	2
2	Authenticating Users from a Credential Service	4
2.1	Use policy builder to add a group of users from a Credential Service (CS) to your AA.....	4
2.2	Use Policy Builder to Modify SAML Configuration	5
2.3	Add a SAML Authentication Server	7
2.4	Enable the Authentication Server	14

Version 2.0.0

1 Setup

1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and HP Select Access 5.2 as an Agency Application (AA). The HP Select Access setup screens are the same, whether setting up an AA or a CS. In section 2, each type of setup is outlined separately. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the main screen shown in Figure 11-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

1.2 Using the Setup Tool

To open the setup tool, go to the HP directory under the Program Files folder; click on the Setup Tool.

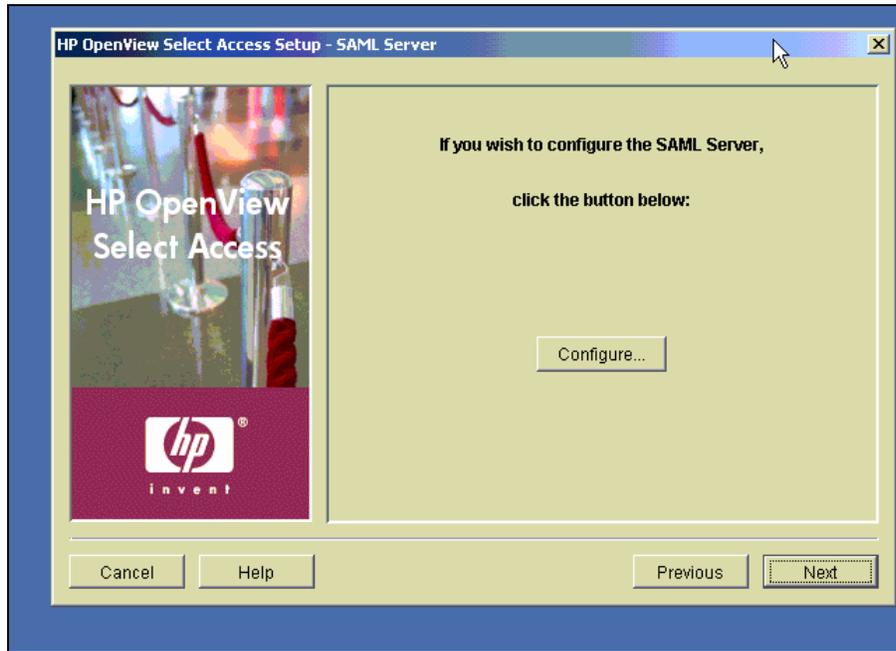


Figure 11-1: Start Setup Tool

Use the setup tool to configure a SAML server. The setup program is the same whether you are setting up a CS or an AA. After the initial setup, do not attempt to use the setup tool again. Instead, use SAML partner properties (See section 2.0 for details) to access properties.

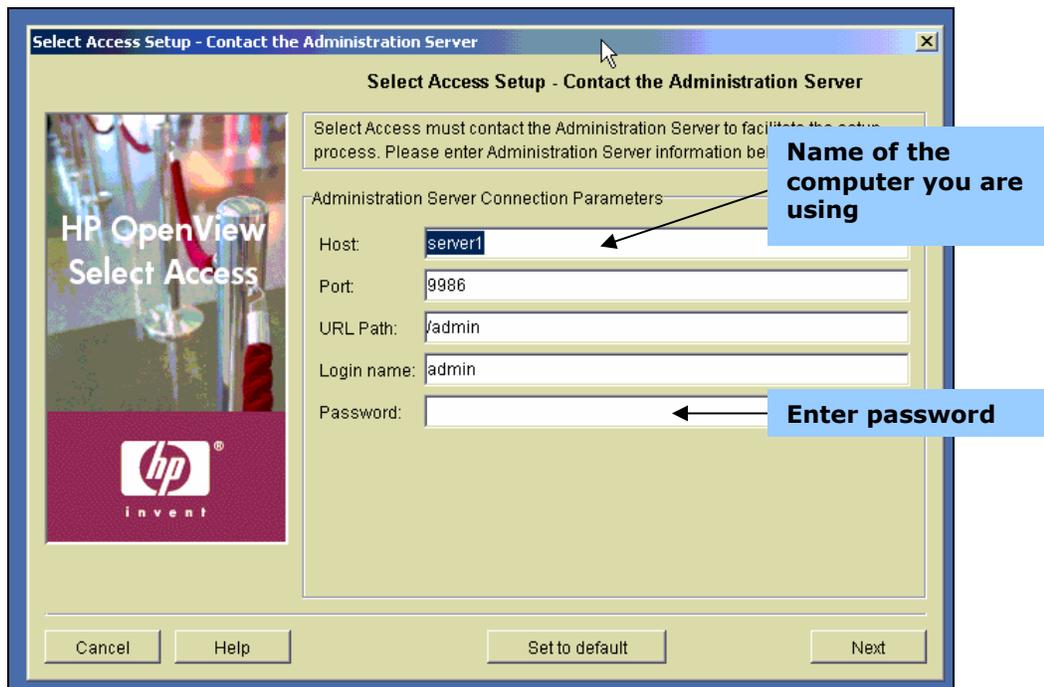


Figure 11-2: Select Access Setup

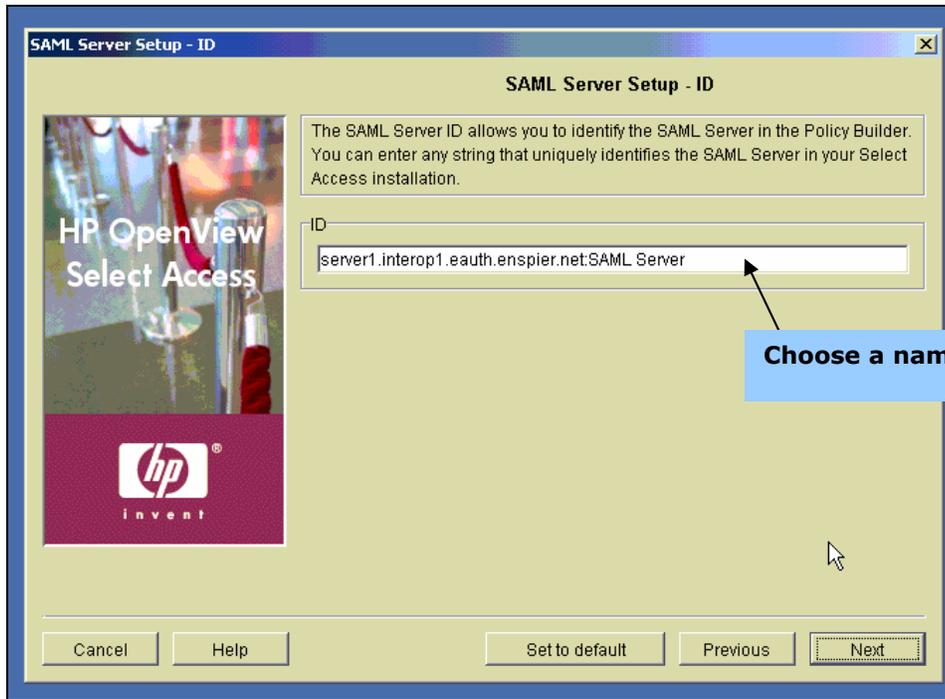


Figure 11-3: Define SAML Server ID

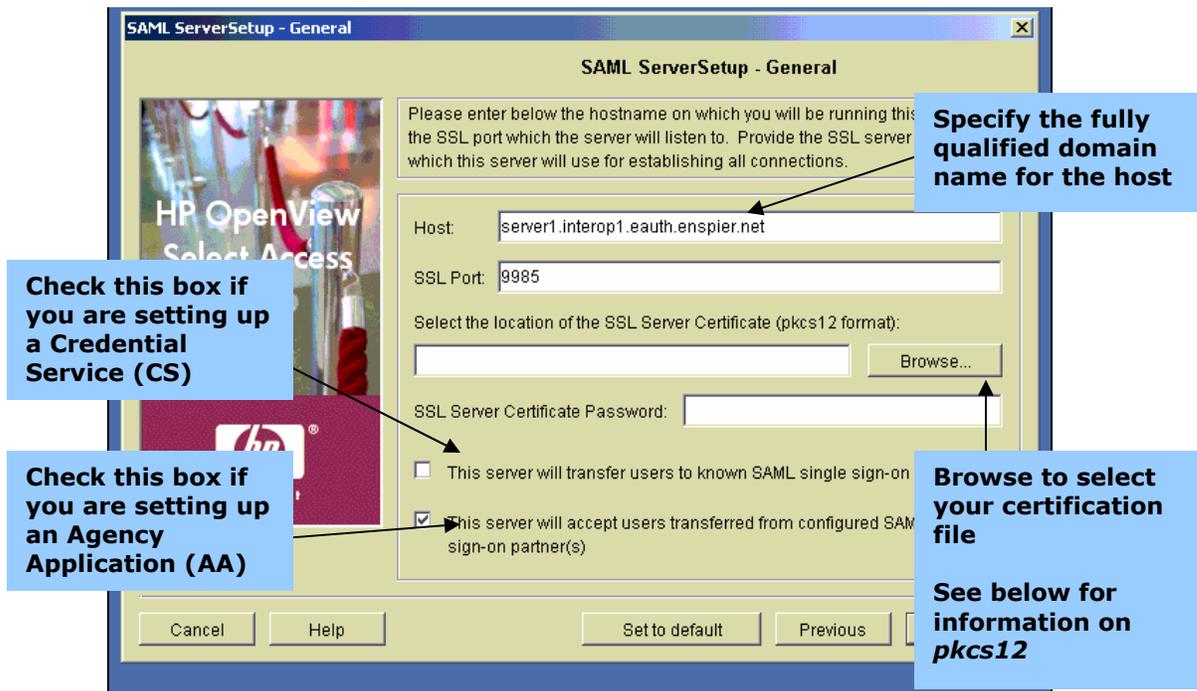


Figure 11-4: General Server Setup

PKCS12 files combine private and public key certificates. The PKCS12 file is protected by a password, which you will provide when you create your PKCS12 file.

2 Authenticating Users from a Credential Service

As an AA that seeks to authenticate users utilizing a certain CS, you must create an authentication server that HP will use to authenticate users. Before you can add a CS, you must create a new group to store user credentials. HP uses a policy matrix to create groups. The following pages will help you use policy matrix, opening a door to HP's user directory.

2.1 Use policy builder to add a group of users from a CS to your AA

First open Policy Builder; go to the Program files folder and open the HP directory. Click on the open view folder, then click on Select Access, then click on Policy Builder.

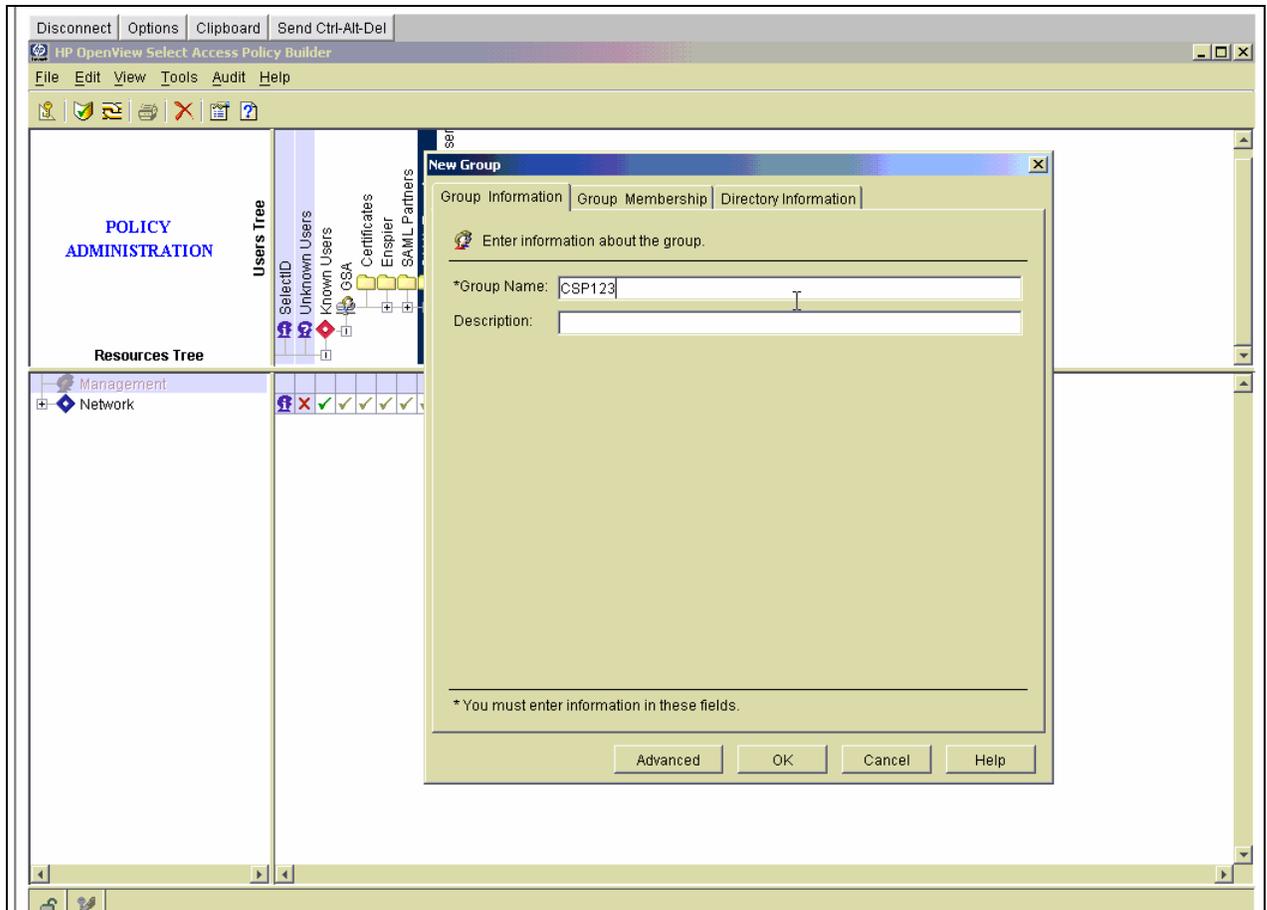


Figure 11-5: Create new CS group

Right click on the folder where you want to store your new group file. Create a new group inside of your known users, where people from your CS will be stored.

2.2 Use Policy Builder to Modify SAML Configuration

After establishing an authentication server, you must configure the SAML partnership for a CS within the authentication server. Use Policy Builder to modify SAML component configuration. To open, go to the Program files folder and open the HP directory. Click on the open view folder, then click on Select Access, then click on Policy Builder. Click on Tools, and then select *Component Configuration*.

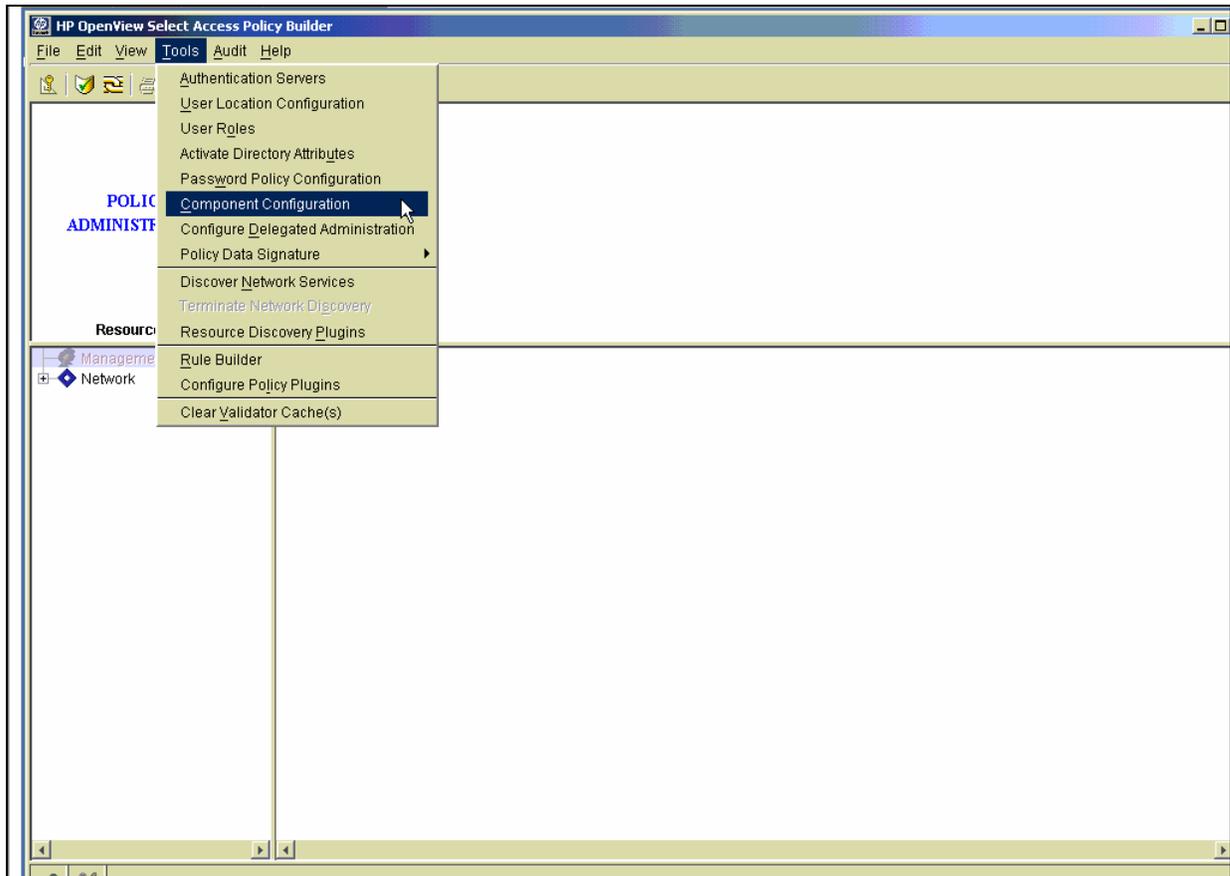


Figure 11-6: Working with Policy Builder

A component configuration window will open, as shown in Figure 11-7 below. To view assertion properties, right click on a SAML server file, choose *Properties*.

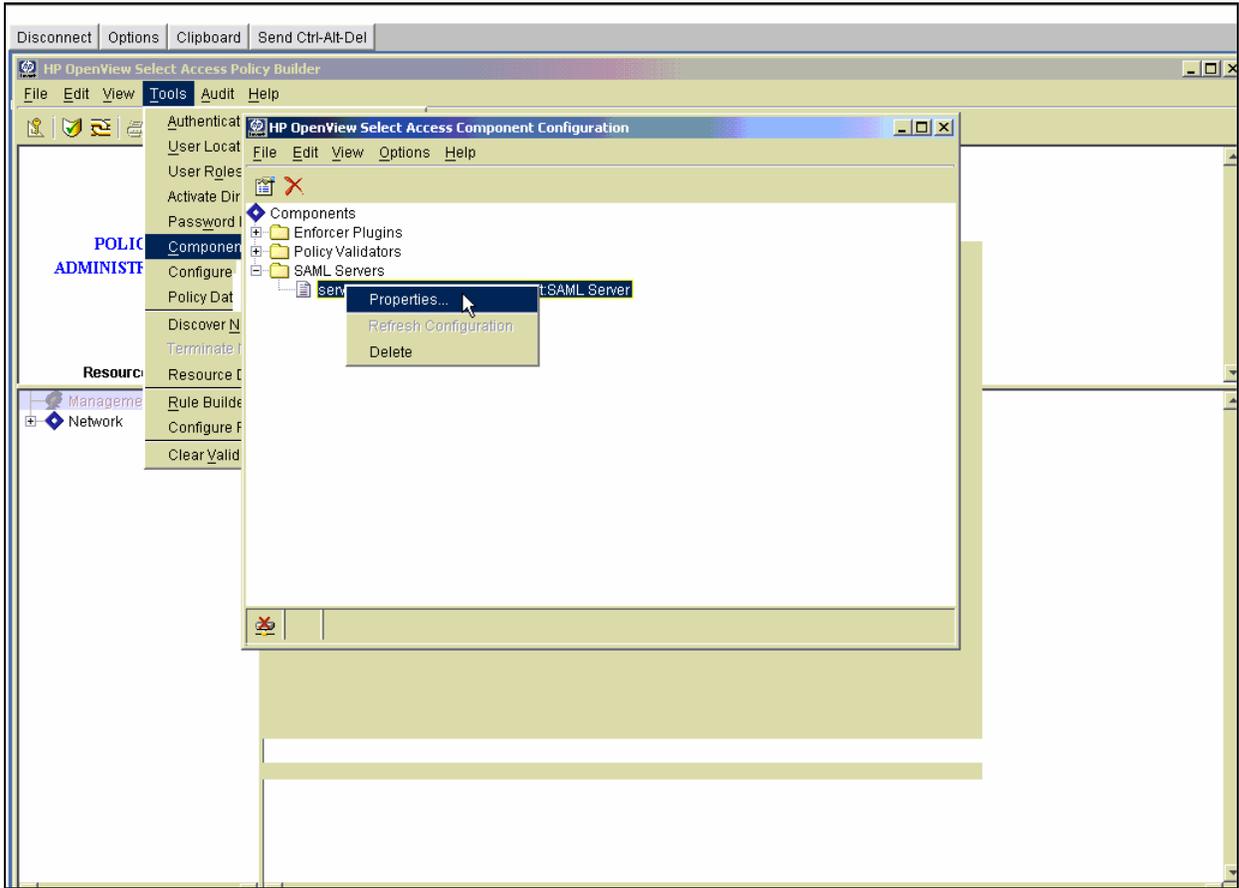


Figure 11-7: Navigating to Component Configuration

2.3 Add a SAML Authentication Server

From the *HP OpenView Select Access Component Configuration* window, open the properties.

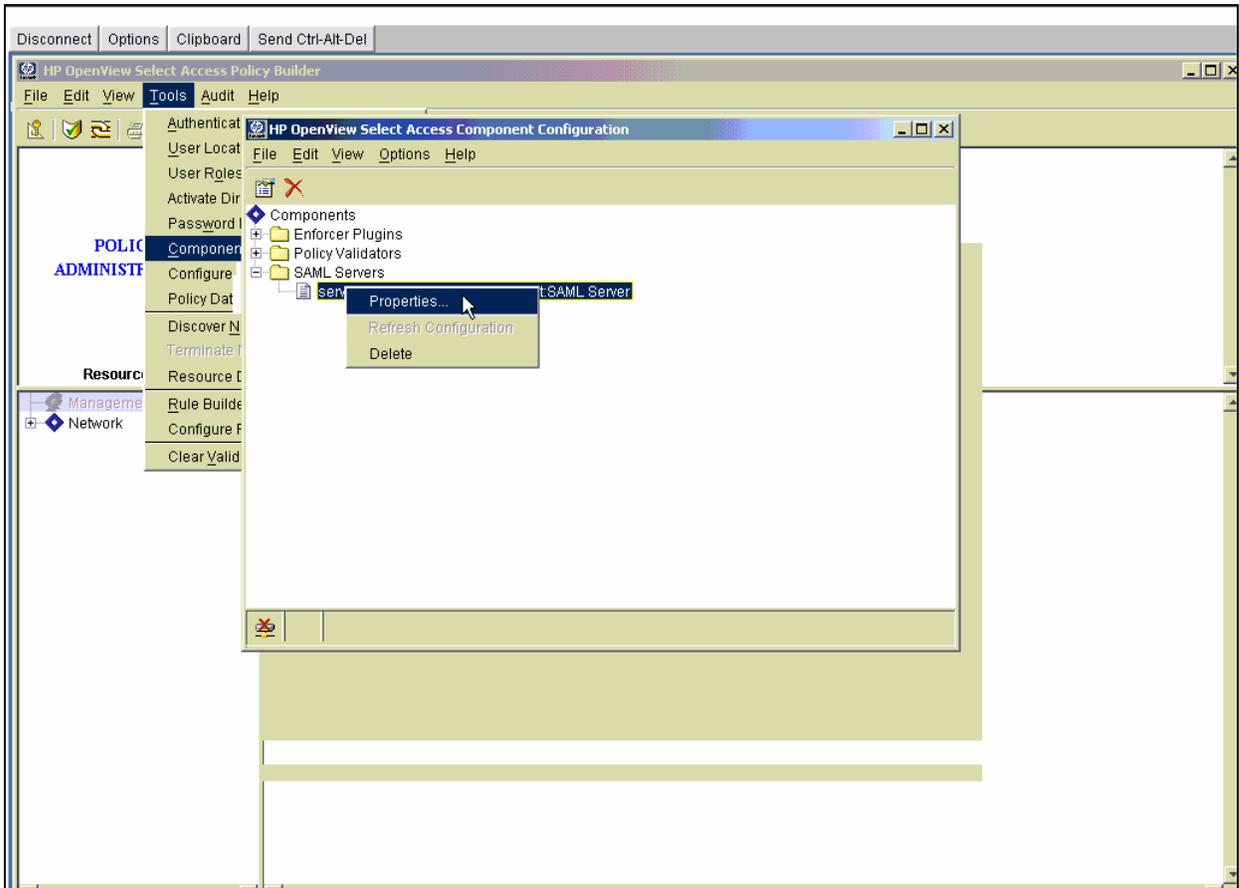


Figure 11-8: Navigate to Properties

After you click on *Properties*, the window shown in Figure 11-9 will open.

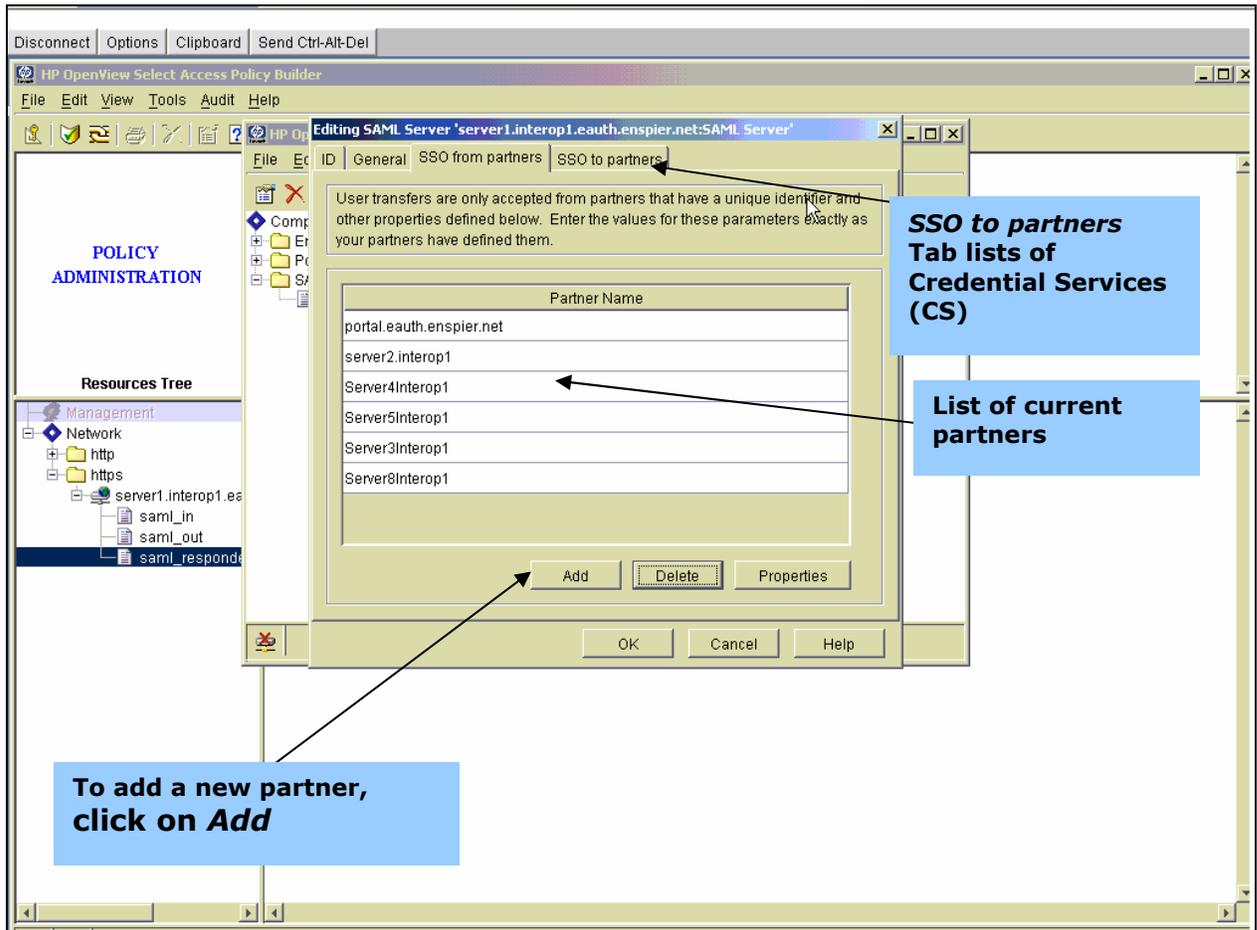


Figure 11-9: Editing the SAML server

After you click on *Add* (See *Figure 11-9*), the *New SAML Authentication Server* window will display. Enter a name, and then click on *Next*.

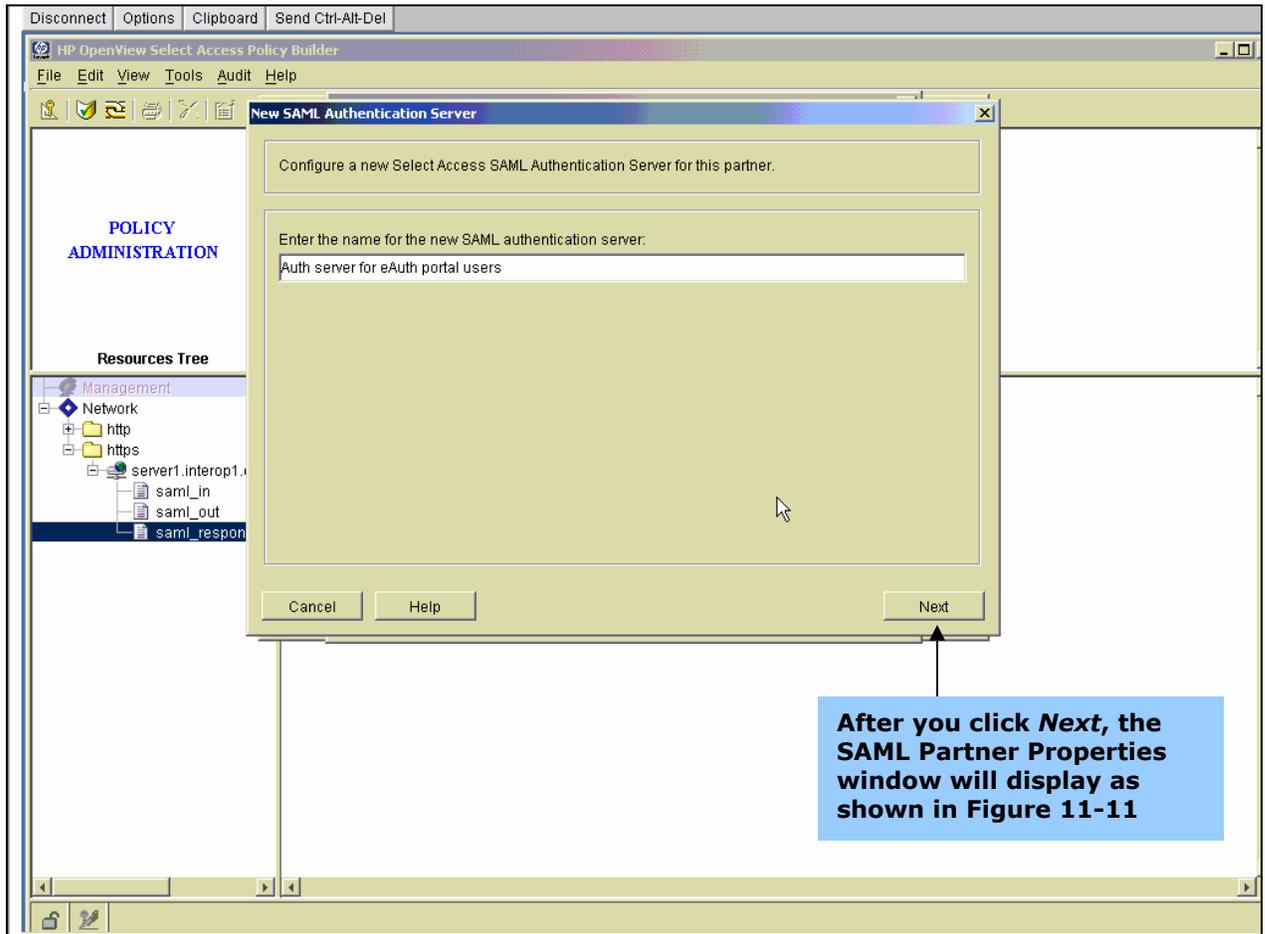


Figure 11-10: Naming new SAML authentication server

Next, enter the partner name. Partner source ID can be obtained from the CS.

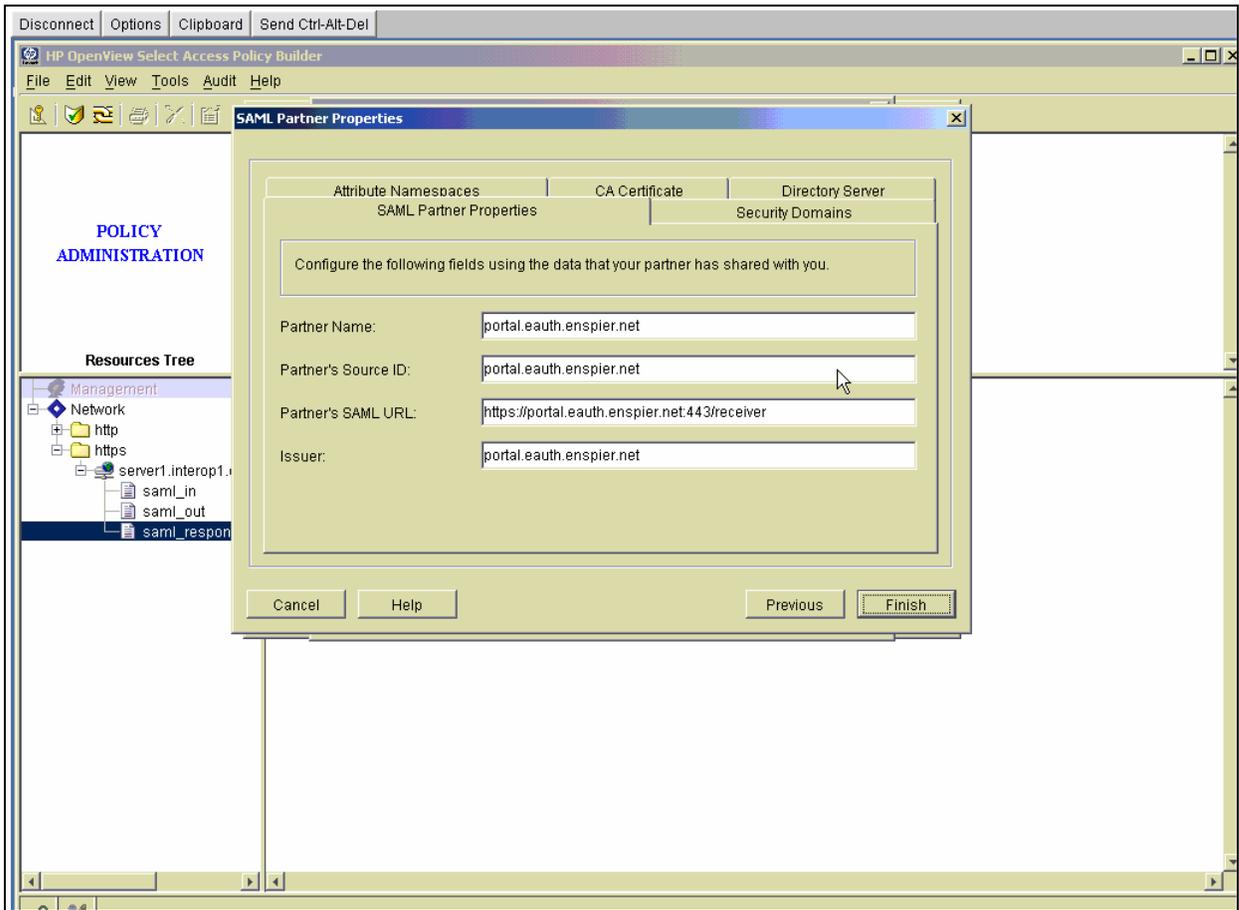


Figure 11-11: SAML partner properties tab

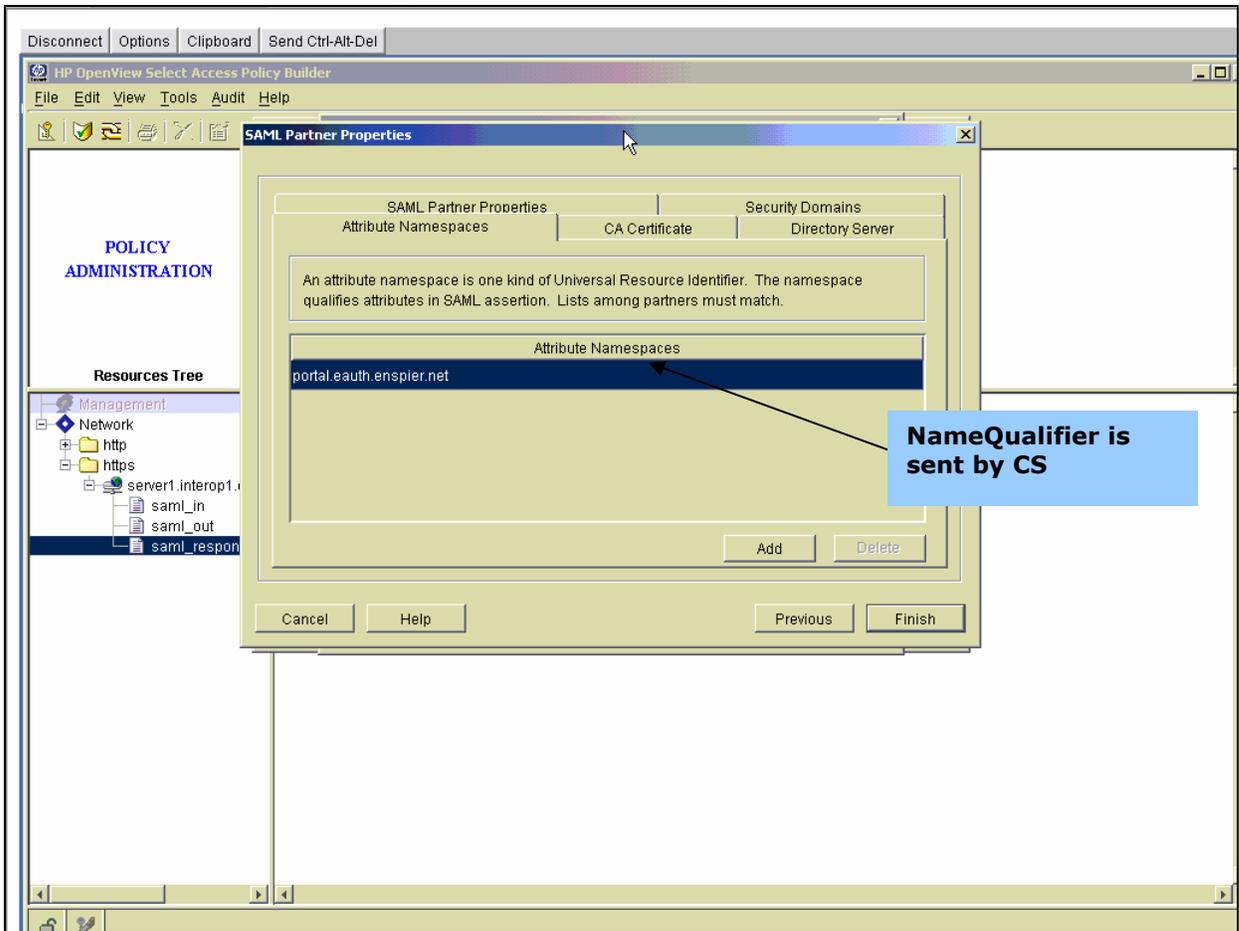


Figure 11-12: Attribute namespace tab

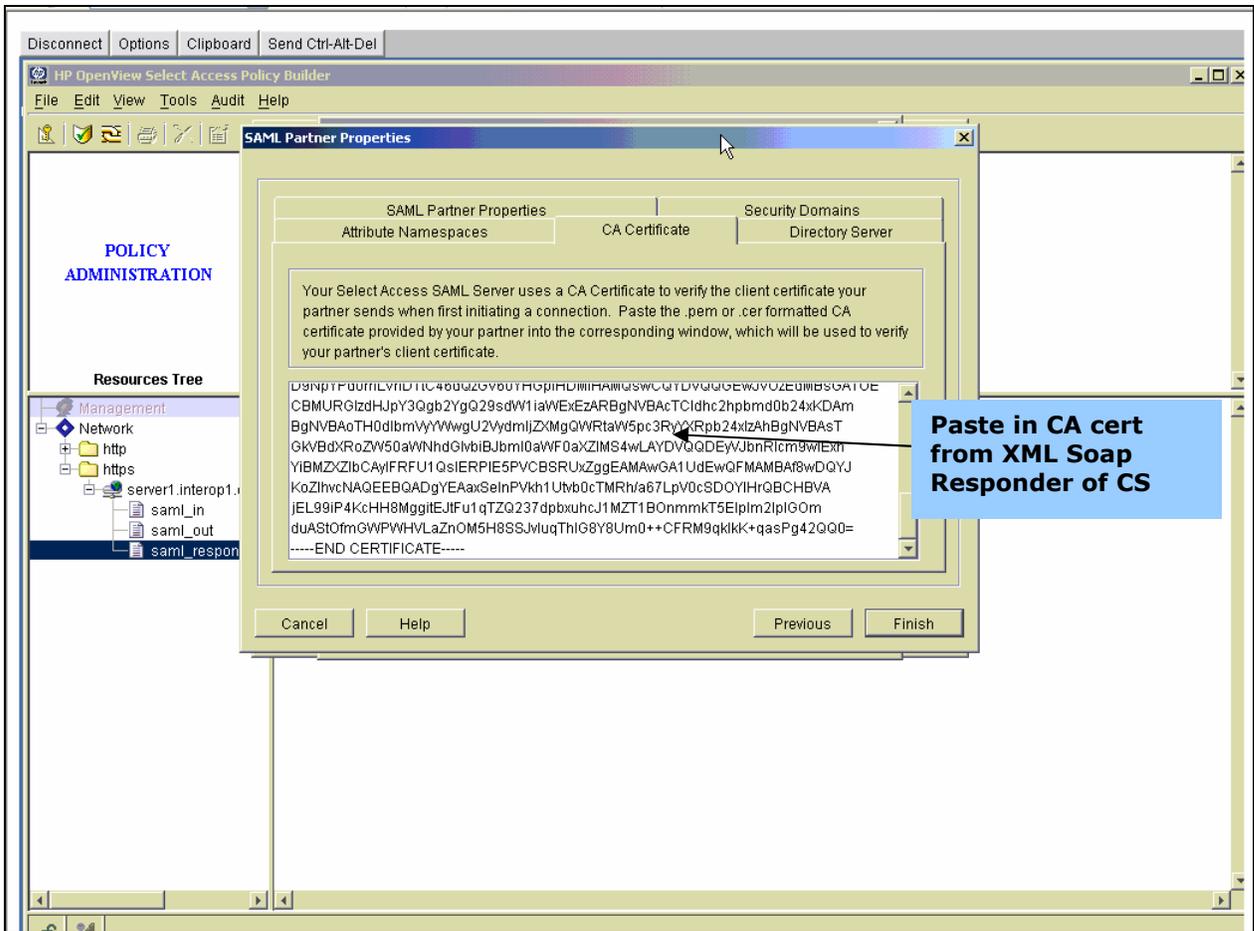


Figure 11-13: CA Certificate tab

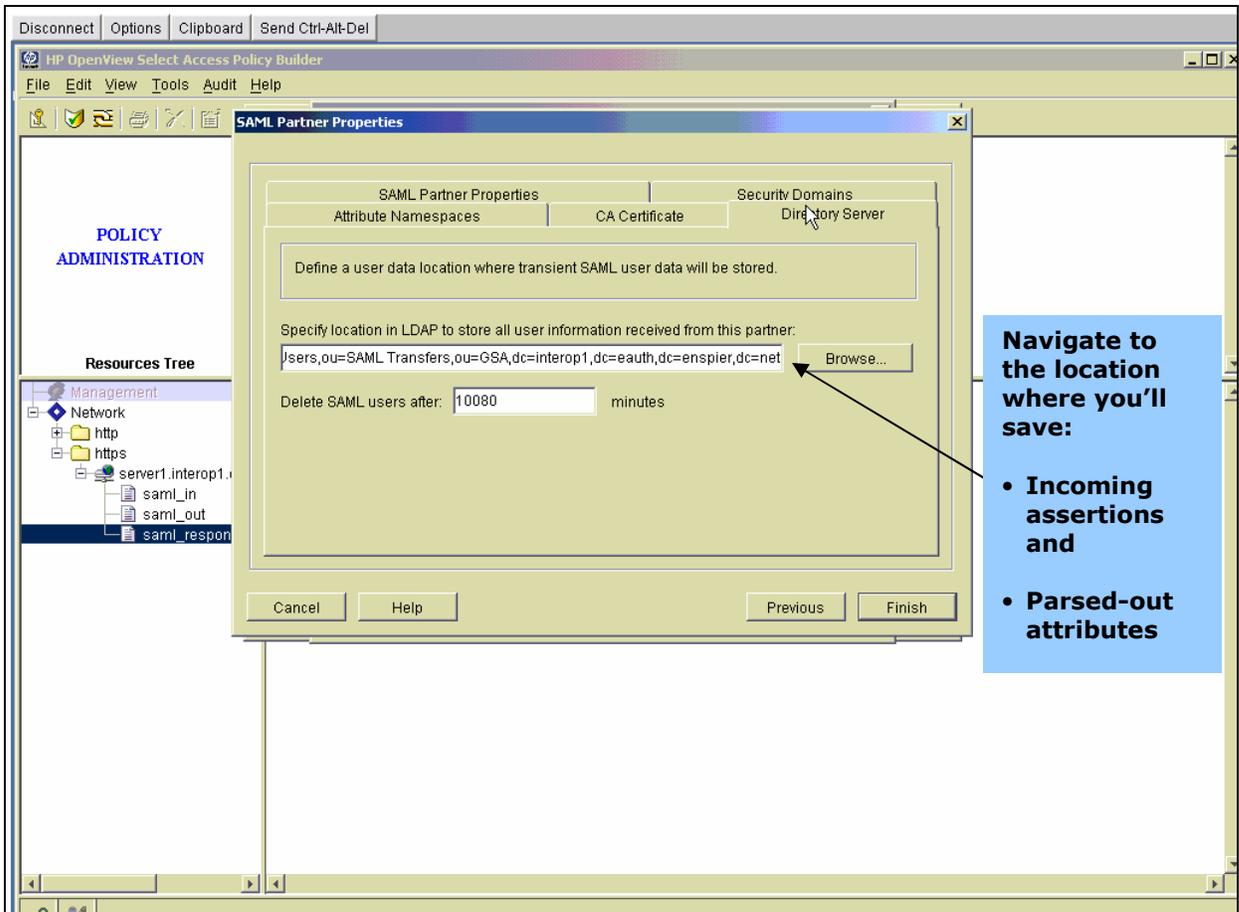


Figure 11-14: Directory server tab

Click on *Finish* when you are done inspecting and editing these tabs.

2.4 Enable the Authentication Server

Modify Select ID properties in order to allocate the desired resources in the resource tree. Use Policy Builder to enable the authentication server. To open, go to the Program files folder and open the HP directory. Click on the open view folder, then click on Select Access, then click on Policy Builder.

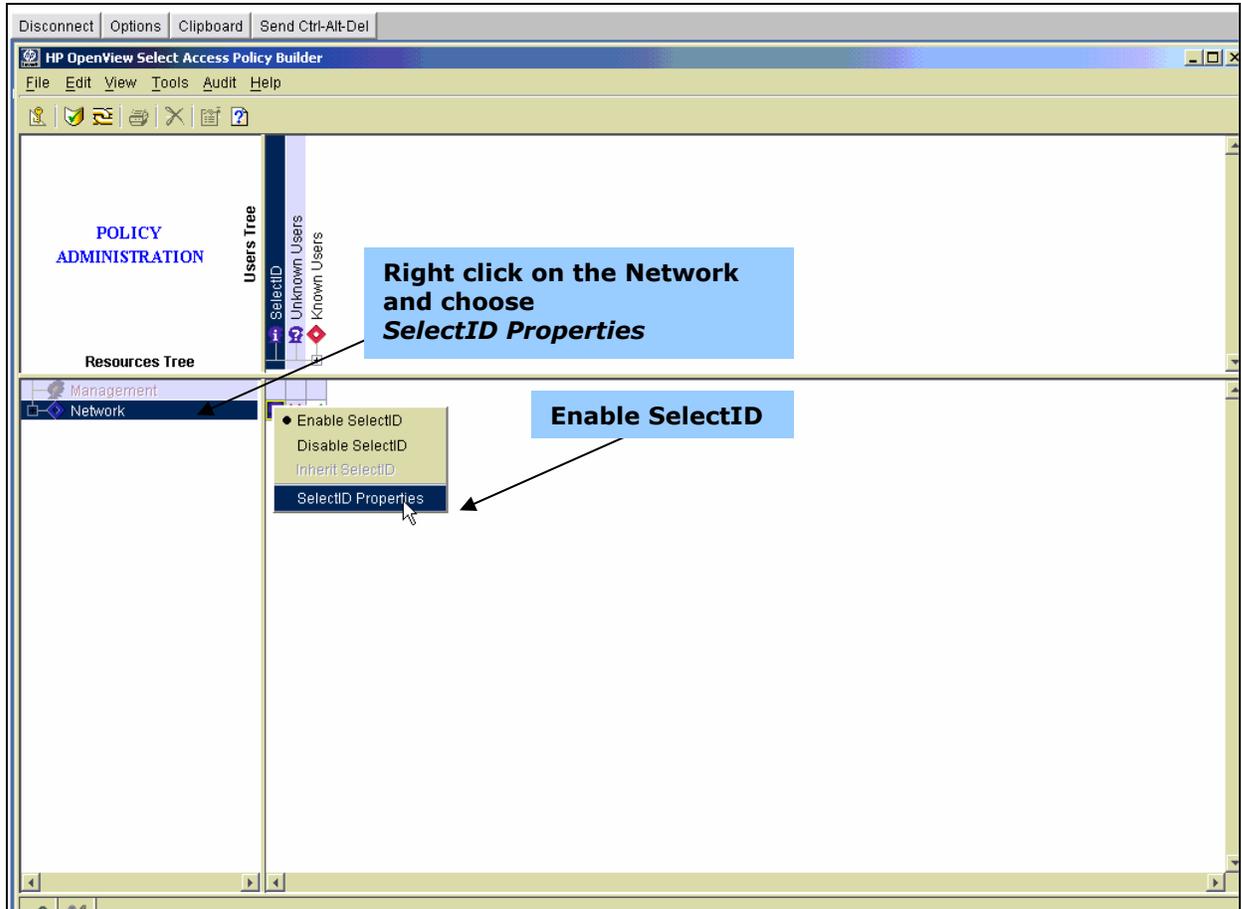


Figure 11-15: Open SelectID Properties

After you choose *SelectID Properties*, the *Authentication Properties* window will open, as shown in Figure 11-16. Use SelectID properties to allow users from this CS access to resources within the resource tree.

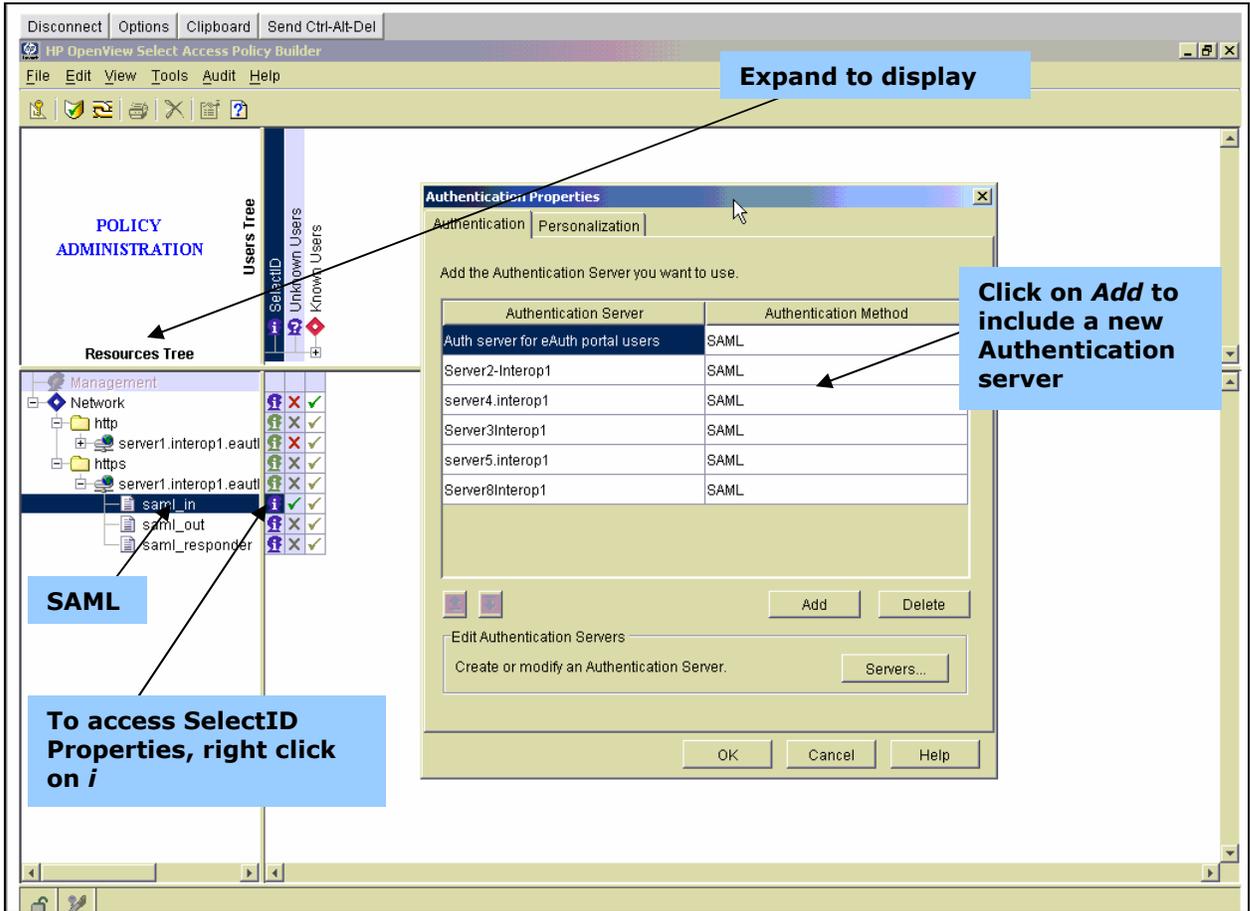


Figure 11-16: Authentication Properties